Exhibit 300: Part I: Summary Information and Justification (All Capital Assets)

I.A. Overview

1. Date of Submission:	12/11/2006
2. Agency:	Department of Justice
3. Bureau:	Federal Bureau of Investigation
4. Name of this Capital Asset:	FBI Terrorist Screening Center (TSC)
5. Unique Project (Investment) Identifier: (For IT investment only, see section 53. For all other, use agency ID system.)	011-10-02-00-01-3177-00
6. What kind of investment will this be in FY2008? (Please NOTE: Investments moving to O&M ONLY in FY2008, with Planning/Acquisition activities prior to FY2008 should not select O&M. These investments should indicate their current status.)	Mixed Life Cycle
7. What was the first budget year this investment was submitted to OMB?	FY2006

8. Provide a brief summary and justification for this investment, including a brief description of how this closes in part or in whole an identified agency performance gap:

The Terrorist Screening Center (TSC) was formed by the Department of Justice in response to Homeland Security Presidential Directive-6 (HSPD-6), dated 16 September 2003. The TSC originates and maintains the US Government's only consolidated terrorist identities database, participates in and explores ways to improve information sharing with all defense, national security, intelligence and law enforcement partners, as well as select foreign partners, and initiates and leads the Federal Search Working Group. The TSC supports national security by providing information on both international and domestic terrorist identities on demand for agencies and/or Departments, including DOS, DHS' Customs and Border Protection and Transportation Security Administration, granting access on the basis of need-to-know to the limit prescribed by the originating agency of record. The TSC's links with many communities, including law enforcement at the state, local, tribal and territorial levels, are maintained around the clock. The TSC's basic philosophy is of information sharing with all partner agencies, and participation in monthly information sharing sessions with partner agencies and foreign government representatives. The TSC hosts regular training for all employees, to include SBU classifications and privacy issues. Despite budget constraints, improvements in efficiency and functionality are ongoing and necessary to obtain the full scope of HSPD-6 and meet the mandate of the President's Management Agenda. The TSC uses the very latest search and retrieval technologies to meet these requirements, and is pioneering search technology in several areas, most notably search standards through development of a control database, search "cocktails" by the use of a combination of multiple search engines, and the federation of searches to search several databases at one time. In BY08, the TSC plans to develop an ability for external users to query the Terrorist Screening Database (TSDB), as well as a portal for external users to better reach and share and exchange information with the TSC call center, intelligence and nominations personnel. The query capability will be in production by early FY08, with the portal to follow. Future efforts will include improved data consumption of NCTC into the TSDB, deployment of biometric capability, planned hardware and software interface with DHS, Voiceprint and DNA data, and improved privacy and security features within EMA supporting TSDB.

9. Did the Agency's Executive/Investment Committee approve this request?	Yes
a. If "yes," what was the date of this approval?	5/19/2006
10. Did the Project Manager review this Exhibit?	Yes
11. Contact information of Project Manager?	
Name	
West, Ed	
Phone Number	703-418-9181
Email	ed.west@tsc.gov
12. Has the agency developed and/or promoted cost effective, energy efficient and environmentally sustainable techniques or practices for this project.	No
a. Will this investment include electronic assets (including computers)?	Yes
b. Is this investment for new construction or major retrofit of a Federal building or facility? (answer applicable to non-IT assets only)	No
1. If "yes," is an ESPC or UESC being used to help fund this investment?	No
2. If "yes," will this investment meet sustainable design principles?	No
3. If "yes," is it designed to be 30% more energy efficient than relevant code?	
13. Does this investment support one of the PMA initiatives?	Yes
If "yes," check all that apply:	Human Capital, Expanded E-Government, Eliminating Improper Payments, R and D Investment Criteria
13a. Briefly describe how this asset directly supports the identified initiative(s)?	The TSC's successes are in direct support of the PMA E-government strategy. Prior to its existence, terrorist screening consisted of manually comparing various spreadsheets and data forms with little communication between Federal, State and Local agencies. The TSC consolidate 12 separate but critical databases tracking terrorist identities into one consolidate Watchlist. That has increased information sharing and created a single point of access for law

	enforcement both here and abroad.
14. Does this investment support a program assessed using the Program Assessment Rating Tool (PART)? (For more information about the PART, visit www.whitehouse.gov/omb/part.)	No
a. If "yes," does this investment address a weakness found during the PART review?	No
b. If "yes," what is the name of the PART program assessed by OMB's Program Assessment Rating Tool?	
c. If "yes," what PART rating did it receive?	
15. Is this investment for information technology?	Yes
If the answer to Question: "Is this investment for information technology?" was "Yes," complete this sub-section. If the answer is "No," do not answer this sub-section.	
For information technology investments only:	
16. What is the level of the IT Project? (per CIO Council PM Guidance)	Level 2
17. What project management qualifications does the Project Manager have? (per CIO Council PM Guidance):	(4) Project manager assigned but qualification status review has not yet started
18. Is this investment identified as "high risk" on the Q4 - FY 2006 agency high risk report (per OMB's "high risk" memo)?	Yes
19. Is this a financial management system?	No
a. If "yes," does this investment address a FFMIA compliance area?	No
1. If "yes," which compliance area:	
2. If "no," what does it address?	
b. If "yes," please identify the system name(s) and system acronym(s) as reported in the most recent financial systems inventory update required by Circular A-11 section 52	
20. What is the percentage breakout for the total FY2008 funding request for the following? (This should total 100%)	
Hardware	18
Software	6

Services	76
Other	0
21. If this project produces information dissemination products for the public, are these products published to the Internet in conformance with OMB Memorandum 05-04 and included in your agency inventory, schedules and priorities?	N/A

22. Contact information of individual responsible for privacy related questions:

Name

Kelley, Patrick W

Phone Number	202-324-8067
Title	Deputy General Counsel/Senior Privacy Officer
E-mail	Patrick.Kelley@ic.fbi.gov
23. Are the records produced by this investment appropriately scheduled with the National Archives and Records Administration's approval?	No

I.B. Summary of Funding

Provide the total estimated life-cycle cost for this investment by completing the following table. All amounts represent budget authority in millions, and are rounded to three decimal places. Federal personnel costs should be included only in the row designated "Government FTE Cost," and should be excluded from the amounts shown for "Planning," "Full Acquisition," and "Operation/Maintenance." The total estimated annual cost of the investment is the sum of costs for "Planning," "Full Acquisition," and "Operation/Maintenance." For Federal buildings and facilities, life-cycle costs should include long term energy, environmental, decommissioning, and/or restoration costs. The costs associated with the entire life-cycle of the investment should be included in this report.

Table 1: SUMMARY OF SPENDING FOR PROJECT PHASES
(REPORTED IN MILLIONS)
(Estimates for BY+1 and beyond are for planning purposes only and do not represent budget decisions)

	PY - 1 and Earlier	PY 2006	CY 2007	BY 2008	BY + 1 2009	BY + 2 2010	BY + 3 2011	BY + 4 and Beyond	Total
Planning									

Budgetary Resources	1.508	4.568	2.942	3.086					
Acquisition									
Budgetary Resources	14.122	59.432	38.28	40.139					
Subtotal Planning & Acquisition									
Budgetary Resources	15.63	64	41.222	43.225					
Operations & Maintenance									
Budgetary Resources	6.405	25.385	16.35	17.145					
TOTAL									
Budgetary Resources	22.035	89.385	57.572	60.37					
Government FTE Costs									
Budgetary Resources	1.105	1.079	1.098	1.117					
Number of FTE represented by Costs:	8	13	13	13					

Note: For the cross-agency investments, this table should include all funding (both managing partner and partner agencies). Government FTE Costs should not be included as part of the TOTAL represented.

2. Will this project require the agency to hire additional FTE's?	No

a. If "yes," How many and in what year?

3. If the summary of spending has changed from the FY2007 President's budget request, briefly explain those changes:

The TSC had to adjust the numbers in the BY08 and out years to reflect DOJ recent pass back, which zeroed out the non-personnel IT enhancement ($6.518M); therefore, the TSC revised the numbers out of the estimates.

I.C. Acquisition/Contract Strategy

1. Complete the table for all (including all non-Federal) contracts and/or task orders currently in place or planned for this investment. Total Value should include all option years for each contract. Contracts and/or task orders completed do not need to be included.

Contracts/Task Orders Table:

Contracts/Task Orders Table

2. If earned value is not required or will not be a contract requirement for any of the contracts or task orders above, explain why:

Per the TSC's briefing to OMB, DOJ and FBI on 5 June 2006 addressing EVM and the ANSI/EIA STD 748 Mr. Dean Hall of DOJ, in an email to the TSC, noted the TSC's Rational Unified Process (RUP) approach was acceptable for managing contract value. The agreement allowed the TSC to deviate from of the ANSI standard and institute cost accounting measures that do not fall within the parameters of the ANSI/EIA standard, while providing the informative elements to the FBI and DOJ necessary for external reporting. The process the TSC instituted was a system tailored to the unique dynamic operational environment the TSC presently operates in, anchored in consistently changing requirements based on external and internal influences, corresponding changes in the baseline, and 13-week delivery cycles, (see Part II, Section C for a sample of this data). To manage activity effectively the TSC instituted the RUP to manage control of projects that requires iterative software development, broken into cycled phases; as well as Agile Project Management using the principles of "scrum" methodology. The TSC produced a Work Breakdown Structure (WBS) and supporting documentation to illustrate TSC activities. The TSC maps the WBS to ongoing operations and maintenance activities and track the finances associated with these efforts; however, because the nature of this work is level-of-effort (LOE), the TSC does not measure this portion of functionality in terms of Earned Value. The WBS accounts for the entire scope of work, and TSC established work packages based on the WBS to plan and track all work. The TSC tracks and measures cost, scheduled activity, and risk for all developmental IT activities with project reporting worksheets maintained by the TSC PMO and revised based on changes within the project. The TSC provides, as needed, a summary of cost and schedule data elements developed from the lowest, manageable level to the program level using the WBS. The process identifies variances, or deviations from the baseline plan, in monthly reporting. The TSC works with the FBI, DOJ, and OMB to verify acceptability of the project management process, and anticipates no changes to the environment and continues to receive new operational requirements from the user community and external parties, enabling the TSC to deliver products in a timely manner that satisfies the user community, increasing operational effectiveness while reducing risk.

3. Do the contracts ensure Section 508 compliance?	N/A
a. Explain why:	TSDB is a sensitive but unclassified (SBU) database not accessible by the public. In addition, TSDB houses sensitive terrorist information and is thus exempt from the requirements of Section 508 of the Rehabilitation Act of 1973; under subsection (a) (5), Exemption for National Security Systems. TSC will ensure, if it arises, that unless it causes an undue burden TSC will make accommodations for Federal employees who are individuals with disabilities to access and use TSC information and data.
4. Is there an acquisition plan which has been approved in accordance with agency requirements?	Yes
a. If "yes," what is the date?	2/18/2006
b. If "no," will an acquisition plan be developed?	
1. If "no," briefly explain why:	

I.D. Performance Information

In order to successfully address this area of the exhibit 300, performance goals must be provided for the agency and be linked to the annual performance plan. The investment must discuss the agency's mission and strategic goals, and performance measures must be provided. These goals need to map to the gap in the agency's strategic goals and objectives this investment is designed to fill. They are the internal and external performance benefits this investment is expected to deliver to the agency

(e.g., improve efficiency by 60 percent, increase citizen participation by 300 percent a year to achieve an overall citizen participation rate of 75 percent by FY 2xxx, etc.). The goals must be clearly measurable investment outcomes, and if applicable, investment outputs. They do not include the completion date of the module, milestones, or investment, or general goals, such as, significant, better, improved that do not have a quantitative or qualitative measure.

Agencies must use Table 1 below for reporting performance goals and measures for all non-IT investments and for existing IT investments that were initiated prior to FY 2005. The table can be extended to include measures for years beyond FY 2006.

Performance Information Table 1:

Fiscal Year	Strategic Goal(s) Supported	Performance Measure	Actual/baseline (from Previous Year)	Planned Performance Metric (Target)	Performance Metric Results (Actual)
2005	Information Technology	Eliminate duplicate records to maintain an accurate list of suspects.	Resolved duplication by writing code for daily ingest process that eliminates multiple records.	100% reduction in duplicate records.	100% reduction achieved with the advent of business rules that inhibit record duplication.
2005	Intelligence	Approved policy standard operating procedures for nominations.	No approves standard operating procedures for nominations.	One set of standard operating procedures.	One set of standard operating procedures completed and 100% monitoring exists.
2005	Information Technology	Maintain 80% of audited records in TSDB.	TSC audits 75% - 80% of all records in the database on suspected individuals.	New technology for will allow task completion by 6/30/2005.	TSC instituted 100% auditing capability as of June 2005.
2005	Information Technology	100% software database ingests in modular form.	Achieved full capability of software ingest for TSC data, captured in modular form.	Develop 100% capability to ingest data in modular form.	Achieve 100% capability to ingest data in modular form.
2006	Partnerships	Document and develop the means to share information quickly through partnering agreements among federal entities.	Develop and execute memorandum agreements (MOA) with other U.S. government agencies in support of TSC where no existed.	Establish MOA with government agencies on an average of one a year to support program objectives.	100% on track with established MOA with DOS for information sharing. Other efforts are in development, some classified in detail.
2006	Partnerships	Document and develop the means to identify agencies for direct access to the TSS database for quick, appropriate and easy data exchange among federal entities.	Develop, at minimum one agreement with another government agency, to allow access to TSC databases where none existed.	Identify agencies and work, on an average of one a year, to institute direct access to TSC data for daily operation.	TBD
2007	Information Technology	Enhance IT Operations in	Develop program to import	Efforts will result in 20% of	TBD

		support of terrorist screening with the use of biometric technologies.	fingerprints and photos for 20% of known or appropriately suspected terrorist into the TSDB with new software developed to support this effort.	the TSDB populated with imported fingerprints markers, as well as links to the IAFIS fingerprint database, and supporting photos of suspects by 9/30/2006.	
2007	Partnerships	Enhance IT Operations in support of terrorist screening though system interfacing technology and agreements	Develop and execute standard interface agreements between TSC and customers where none existed.	Establish interfaces with customers on average of one a year to provide information from the TSDB.	TBD
2008	Intelligence	Share information quickly, easily and appropriately among federal and foreign entities through agreements and data exchange.	Institute TSC services with foreign partners, based on agreements that were not in place prior.	TSC services have been 100% established with present foreign partners by 9/30/2007.	TBD
2008	Records Management	Provide reliable, trusted, and cost-effective IT services in support of managing and improving screening technology.	Develop capability to match identities with photos and/or fingerprints with software that did not exist prior.	TSC institutes 10% success rate for data exports to include photos and/or fingerprints by 9/30/2007.	TBD
2009	Information Technology	Enhance IT Operations in support of terrorist screening with additional R&D efforts in anonymous data sorting.	Increase TSC's ability to screen against TSC data using anonymous hashing techniques with Government organizations based on R&D efforts from the federal working group.	Provide on average of one customer a year (100%) the ability to screen data using anonymous hashing techniques	TBD
2009	Partnerships	Share information quickly, easily and appropriately among federal entities on a multi-level platform.	Improve TSC's ability to implement multi-level interfaces among U.S. Government organizations where none existed.	Provide an average of two interfaces a year (100%) with customer agencies to establish identity vetting procedures.	TBD
2010	Information Technology	Enhance IT Operations in support of terrorist screening with new software opportunities.	TSC provide customers the ability to operate data at multiple classification levels with new software to support this objective.	TSC institutes 100% capability for all customers to operate at three classification levels by 9/30/2008.	TBD
2010	Information Technology	Secure and protect information among Federal	TSC integrates internal operation systems for	TSC works to integrate two operational systems among	TBD

		organizations through the continuous efforts of establishing interface agreements among additional agencies.	Government agencies to improve data capabilities, based on new software developed in support of this effort.	Government customers yearly until complete.	
2011	Information Technology	Enhance IT Operations in support of terrorist screening among Federal entities with various classification.	The ability to create and operate inter-connected networks at various classification levels, which did not exist prior.	TSC will work annually to integrate two system networks with different classification levels until complete, the first to be completed by 9/30/2008.	TBD
2011	Partnerships	Enhance IT Operations in support of terrorist screening between Federal and private sector organizations.	TSC needs to increase support for private sector screening, which does not exist due to sensitivity of data and non-existing agreements.	TSC, through DHS, will support efforts to connect with private industry for sector screening on average of two per year (100%).	TBD
2012	Counterterrorism	Continue and enhance IT Operations in support of terrorist screening among all Federal entities and foreign partners by direct access.	TSC customers need to have an improved ability to access databases directly, which did not exist prior.	TSC will successfully access two customer databases (100%) by 9/30/2009.	TBD
2012	Information Technology	Enhance IT Operations in support of terrorist screening through improved data functionality and operations.	TSC is working to increase the number of service organizations by 25% in order to improve data functionality, improving operations of screening.	By 9/30/2009, TSC will begin to implement on average of one service organization per year (100%) data screen linking.	TBD

All new IT investments initiated for FY 2005 and beyond must use Table 2 and are required to use the Federal Enterprise Architecture (FEA) Performance Reference Model (PRM). Please use Table 2 and the PRM to identify the performance information pertaining to this major IT investment. Map all Measurement Indicators to the corresponding "Measurement Area" and "Measurement Grouping" identified in the PRM. There should be at least one Measurement Indicator for at least four different Measurement Areas (for each fiscal year). The PRM is available at www.egov.gov.

Performance Information Table 2:

Fiscal Year	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Planned Improvement to the Baseline	Actual Results

I.E. Security and Privacy

In order to successfully address this area of the business case, each question below must be answered at the system/application level, not at a program or agency level. Systems supporting this investment on the planning and operational systems security tables should match the systems on the privacy table below. Systems on the Operational Security Table must be included on your agency FISMA system inventory and should be easily referenced in the inventory (i.e., should use the same name or identifier).

All systems supporting and/or part of this investment should be included in the tables below, inclusive of both agency owned systems and contractor systems. For IT investments under development, security and privacy planning must proceed in parallel with the development of the system/s to ensure IT security and privacy requirements and costs are identified and incorporated into the overall lifecycle of the system/s.

Please respond to the questions below and verify the system owner took the following actions:

1. Have the IT security costs for the system(s) been identified and integrated into the overall costs of the investment:	Yes
a. If "yes," provide the "Percentage IT Security" for the budget year:	3.83
2. Is identifying and assessing security and privacy risks a part of the overall risk management effort for each system supporting or part of this investment.	Yes

3. Systems in Planning - Security Table:

Name of System	Agency/ or Contractor Operated System?	Planned Operational Date	Planned or Actual C&A Completion Date
TSC OWTCI	Government Only	12/1/2006	5/1/2006

4. Operational Systems - Security Table:

Name of System	Agency/ or Contractor Operated System?	NIST FIPS 199 Risk Impact level	Has C&A been Completed, using NIST 800-37?	Date C&A Complete	What standards were used for the Security Controls tests?	Date Complete(d): Security Control Testing	Date the contingency plan tested
TSCNET	Government Only		Yes	4/26/2005	FIPS 200 / NIST 800-53	5/5/2006	9/28/2006

5. Have any weaknesses related to any of the systems part of or supporting this investment been identified by the agency or IG?

a. If "yes," have those weaknesses been incorporated agency's plan of action and milestone process?

6. Indicate whether an increase in IT security funding is requested to remediate IT security weaknesses?

a. If "yes," specify the amount, provide a general description of the weakness, and explain how the funding request will remediate the weakness.

7. How are contractor security procedures monitored, verified, validated by the agency for the contractor systems above?

Not Applicable

8. Planning & Operational Systems - Privacy Table:

Name of System	Is this a new system?	Is there a Privacy Impact Assessment (PIA) that covers this system?	Is the PIA available to the public?	Is a System of Records Notice (SORN) required for this system?	Was a new or amended SORN published in FY 06?
TSC OWTCI	Yes	No.	No, because a PIA is not yet required to be completed at this time.	Yes	No, because the existing Privacy Act system of records was not substantially revised in FY 06.
TSCNET	No	No.	No, because a PIA is not yet required to be completed at this time.	Yes	No, because the existing Privacy Act system of records was not substantially revised in FY 06.

I.F. Enterprise Architecture (EA)

In order to successfully address this area of the business case and capital asset plan you must ensure the investment is included in the agency's EA and Capital Planning and Investment Control (CPIC) process, and is mapped to and supports the FEA. You must also ensure the business case demonstrates the relationship between the investment and the business, performance, data, services, application, and technology layers of the agency's EA.

1. Is this investment included in your agency's target enterprise architecture?	Yes
a. If "no," please explain why?	
2. Is this investment included in the agency's EA Transition Strategy?	Yes
a. If "yes," provide the investment name as identified in the Transition Strategy provided in the agency's most recent annual EA Assessment.	Terrorist Screening System (TSS)
b. If "no," please explain why?	

3. Service Reference Model (SRM) Table:

Identify the service components funded by this major IT investment (e.g., knowledge management, content management, customer relationship management, etc.). Provide this information in the format of the following table. For detailed guidance regarding components, please refer to http://www.whitehouse.gov/omb/egov/.

Agency Component Name	Agency Component Description	Service Domain	FEA SRM Service Type	FEA SRM Component	FEA Service Component Reused Name	FEA Service Component Reused UPI	Internal or External Reuse?	BY Funding Percentage
		Back Office Services	Asset / Materials Management	Computers / Automation Management			No Reuse	8
		Back Office Services	Data Management	Data Warehouse			No Reuse	9
		Back Office Services	Development and Integration	Data Integration			No Reuse	8
		Business Analytical Services	Visualization	Mapping / Geospatial / Elevation / GPS			No Reuse	3
		Business Management Services	Management of Processes	Requirements Management			No Reuse	15
		Customer Services	Customer Relationship Management	Call Center Management			No Reuse	12
		Digital Asset Services	Knowledge Management	Information Sharing			No Reuse	7
		Digital Asset Services	Knowledge Management	Knowledge Distribution and Delivery			No Reuse	12
Identity Resolution	Recording of the Nominations Decisions	Digital Asset Services	Knowledge Management	NEW			No Reuse	7
		Support Services	Search	Query			No Reuse	6
		Support Services	Security Management	Identification and Authentication			No Reuse	13

Use existing SRM Components or identify as "NEW". A "NEW" component is one not already identified as a service component in the FEA SRM.

A reused component is one being funded by another investment, but being used by this investment. Rather than answer yes or no, identify the reused service component funded by the other investment and identify the other investment using the Unique Project Identifier (UPI) code from the OMB Ex 300 or Ex 53 submission.

'Internal' reuse is within an agency. For example, one agency within a department is reusing a service component provided by another agency within the same department. 'External' reuse is one agency within a department reusing a service component provided by another agency in another department. A good example of this is an E-Gov initiative service being reused by multiple organizations across the federal government.

Please provide the percentage of the BY requested funding amount used for each service component listed in the table. If external, provide the funding level transferred to another agency to pay for the service.

4. Technical Reference Model (TRM) Table:

To demonstrate how this major IT investment aligns with the FEA Technical Reference Model (TRM), please list the Service Areas, Categories, Standards, and Service Specifications supporting this IT investment.

FEA SRM Component	FEA TRM Service Area	FEA TRM Service Category	FEA TRM Service Standard	Service Specification (i.e. vendor or product name)
NEW	Component Framework	Data Management	Database Connectivity	IBM; Entity Resolution- version 1.0
NEW	Component Framework	Data Management	Database Connectivity	The Analysis Corp.; Advanced Search -Version 0.5 (still under partial development)
Knowledge Distribution and Delivery	Component Framework	Data Management	Reporting and Analysis	Business Objects SA; Crystal Reports-version 9.0
Query	Component Framework	Data Management	Reporting and Analysis	Chiliad; Chiliad Discovery- version 3.7
Mapping / Geospatial / Elevation / GPS	Component Framework	Data Management	Reporting and Analysis	Environmental Systems Research Institute (ESRI); ArcView, version 9.0
Mapping / Geospatial / Elevation / GPS	Component Framework	Data Management	Reporting and Analysis	ESRI, MapObjects-version 9.0
Mapping / Geospatial / Elevation / GPS	Component Framework	Data Management	Reporting and Analysis	Oracle; Toplink: version 10g release 3(10.1.3.0)
Knowledge Distribution and Delivery	Component Framework	Data Management	Reporting and Analysis	Reporting Engines; Formula One's- version 2.2.
Query	Component Framework	Data Management	Reporting and Analysis	The Analysis Corp., Inc. (TAC); Celatro-version 2.1
Identification and	Component Framework	Security	Supporting Security	Check Point /Source Fire; intrusion & detection-version

Authentication			Services	3D(Solaris 8.0 compatibility)
Identification and Authentication	Component Framework	Security	Supporting Security Services	CISCO; Pix Virtual Firewalls ¿version 7.0
Identification and Authentication	Component Framework	Security	Supporting Security Services	Entrust; Public Key Infrastructure, Version 6.0
Identification and Authentication	Component Framework	Security	Supporting Security Services	Lockheed Martin; Security Exchange-One Way Transfer- version 1.0
Identification and Authentication	Component Framework	Security	Supporting Security Services	Symantec Gateway (Firewalls) version 5420
Knowledge Distribution and Delivery	Service Access and Delivery	Delivery Channels	Extranet	MITRE/TKC Communications; TSCNet-version 2
Identification and Authentication	Service Access and Delivery	Service Requirements	Authentication / Single Sign-on	Oracle; Data Base 10g-version 10.2
Call Center Management	Service Access and Delivery	Service Transport	Supporting Network Services	TAC; Encounter Management Application-version 2.0
Information Sharing	Service Interface and Integration	Integration	Enterprise Application Integration	IBM; IBM Websphere MQ -version 6.0
Data Integration	Service Interface and Integration	Integration	Enterprise Application Integration	TAC; J2EE (EJB, JavaScript) ¿version 4.1.2
Information Sharing	Service Interface and Integration	Integration	Enterprise Application Integration	TSC (GOTS Product);Encounter Management Application ¿version 2.0
Computers / Automation Management	Service Platform and Infrastructure	Delivery Servers	Portal Servers	IBM; IBM Websphere Process Server -version 6.0 (tentative selection)
Requirements Management	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	IBM; Rational Clear Case-version 6.0

Service Components identified in the previous question should be entered in this column. Please enter multiple rows for FEA SRM Components supported by multiple TRM Service Specifications

In the Service Specification field, Agencies should provide information on the specified technical standard or vendor product mapped to the FEA TRM Service Standard, including model or version numbers, as appropriate.

5. Will the application leverage existing components and/or applications across the Government (i.e., FirstGov, Pay.Gov, etc)? No

a. If "yes," please describe.

6. Does this investment provide the public with access to a government automated information system?	No
a. If "yes," does customer access require specific software (e.g., a specific web browser version)?	
1. If "yes," provide the specific product name(s) and version number(s) of the required software and the date when the public will be able to access this investment by any software (i.e. to ensure equitable and timely access of government information and services).	

Exhibit 300: Part II: Planning, Acquisition and Performance Information

II.A. Alternatives Analysis

Part II should be completed only for investments identified as "Planning" or "Full Acquisition," or "Mixed Life-Cycle" investments in response to Question 6 in Part I, Section A above.

In selecting the best capital asset, you should identify and consider at least three viable alternatives, in addition to the current baseline, i.e., the status quo. Use OMB Circular A- 94 for all investments, and the Clinger Cohen Act of 1996 for IT investments, to determine the criteria you should use in your Benefit/Cost Analysis.

1. Did you conduct an alternatives analysis for this project?	Yes
a. If "yes," provide the date the analysis was completed?	9/1/2004
b. If "no," what is the anticipated date this analysis will be completed?	10/31/2006
c. If no analysis is planned, please briefly explain why:	

2. Alternative Analysis Results:

Use the results of your alternatives analysis to complete the following table:

Send to	Alternative Analyzed	Description of Alternative	Risk Adjusted Lifecycle Costs	Risk Adjusted Lifecycle

OMB			estimate	Benefits estimate
True	3 - Do incremental development on an existing watchlisting GOTS product.	Allows the TSC to utilize an existing GOTS watchlisting system (TIPOFF), in use at the TTIC, by the company (TAC) supporting TTIC, by a company in the watchlisting business for years supporting the Department of State, a partner of TSC, and was the baseline repository for terrorist identity information. This option allowed TSC to leverage technical staff with an extensive knowledge of the watchlisting, the TIPOFF system, and mitigate risk by doing incremental development on a proven platform.	151.9	0

3. Which alternative was selected by the Agency's Executive/Investment Committee and why was it chosen?

Alternative 3 was selected due to the rapid response required by HSPD-6, leveraging existing GOTS product (TIPOFF) with available Commercial-Off-The-Shelf products to obtain optimal results. In so doing, the TSC decreased cost and lead time needed to modify an existing capability. The TSC also leveraged existing IT resources that understood the product tool's capability and high-level requirements to allow the TSC to account for development of the system in a manner acceptable for the users.

4. What specific qualitative benefits will be realized?

The TSC process supports recommendations from the 9/11 Commission, HSPD-6 and 11, Executive Order No. 13356, Non-Governmental Organization Vetting, the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 and Private Sector Screening, all of which will help to prevent another attack such as the one that occurred on September 11, 2001. As a result, the TSC managed over 82,000 potential encounters with known or suspected terrorists in only 35 months of operation. Over 9,000 of those encounters occurred outside the US, before terrorist ever had a chance to enter the United States. Over 45,000 of those encounters occurred at the border, and of those more than 28,000 that occurred in the interior of the US for the first time: federal, state, local, territorial and tribal law enforcement officers had the ability to know if they had encountered a known or suspected terrorist; and they were directed by the FBI's Counterterrorism Division regarding exactly what action to take. As the sole source for the United States Government official consolidated watch list, the TSC links and manages information on suspected terrorist obtained from the National Counterterrorism Center (NCTC) and the Federal Bureau of Investigation (FBI); and exported to multiple agencies under multiple Departments. Due to the amount of time allotted to implement the TSC upon signing of HSPD-6, the TSC formulated a rapid solution to integrate what historically were separate watch lists and analytical centers across the law enforcement and intelligence communities. By merging these valuable assets into a common, single information source, the Government increases overall efficiency at identifying potential terrorists and reduce cost and work of multiple IT efforts used in the past prior to the consolidation of hardware, technology, and resources. The other alternatives did not provide significant benefits as they required either the use of proprietary software that would have resulted in major fixes in the future, agreements for modification that would delay the start-up of the organization, an extreme learning curve among the commercial developers, additional costs that could not be supported with the limited funding available for start-up, and in the case of one alternative, a lack of experience in this field of work that would have been detrimental to cost and schedule delivery that would be, at minimum, six months behind.

II.B. Risk Management

You should have performed a risk assessment during the early planning and initial concept phase of this investment's life-cycle, developed a risk-adjusted life-cycle cost estimate and a plan to eliminate, mitigate or manage risk, and be actively managing risk throughout the investment's life-cycle.

1. Does the investment have a Risk Management Plan?	Yes
a. If "yes," what is the date of the plan?	1/31/2006
b. Has the Risk Management Plan been significantly changed since last year's submission to OMB?	Yes

c. If "yes," describe any significant changes:

The revision to the TSC Risk Management Plan now incorporates a revised risk management matrix that captures informational elements that map to the DOJ dashboard reporting tool, including the risk impact, priority, impact time frame and horizon. Additionally, the matrix uses the determination of the probability of exposure and severity of impact to determine the risk exposure of each one assessed. Finally, the plan addresses the use of the Borda algorithm in the event a number of risks measure the same. Outlined in the response for Question 3 in this section are details of how the organization addresses risks.

2. If there currently is no plan, will a plan be developed?	
a. If "yes," what is the planned completion date?	
b. If "no," what is the strategy for managing the risks?	

3. Briefly describe how investment risks are reflected in the life cycle cost estimate and investment schedule:

The TSC measures risk, based on the organization's inability to achieve overall program objectives within defined program requirements and constraints. All risks are comprised of three components: the probability of occurrence, the impact of the risk to the program, and the time horizon during which notes what consequences will occur without if mitigation of risks does not take place. TSC identifies and manages risk by using a Risk Management Matrix (RMM) to compile risk data, and takes appropriate actions to mitigate them. TSC collects data and reflects the life cycle cost estimates in project reports, and balances these against the risks identified. The TSC uses the RMM to determine the priority of each risk for action, and as the tool to report risks regularly. While the TSC manages risk, there is a very low risk associated with most projects due to the short life cycle and the use of time and materials contracts supporting their development. The TSC leverages cost risks by diverting level of effort to priority projects, without impacting cost of the projects from which the TSC divert resources; the greatest impact is to schedule. However, most systems under development for replacing existing systems have a high degree of effectiveness inherent in their existing product, and the TSC gains efficiency with delivery of the new product. Therefore, schedule risks are generally low as well with diversion of level of effort. For example, delays to one project may be due to the need to divert resources to another priority project. While the delivery schedule may be impacted, the TSC does not expend costs on the project until it re-prioritization occurs for delivery. However, in the meantime, the existing system still has effective use.

II.C. Cost and Schedule Performance

1. Does the earned value management system meet the criteria in ANSI/EIA Standard-748?	No

2. Answer the following questions about current cumulative cost and schedule performance. The numbers reported below should reflect current actual information. (Per OMB requirements Cost/Schedule Performance information should include both Government and Contractor Costs):

a. What is the Planned Value (PV)?	15760
b. What is the Earned Value (EV)?	12890
c. What is the actual cost of work performed (AC)?	14000
d. What costs are included in the reported Cost/Schedule Performance information (Government Only/Contractor Only/Both)?	Contractor Only
e. "As of" date:	11/30/2006
3. What is the calculated Schedule Performance Index (SPI= EV/PV)?	0.82
4. What is the schedule variance (SV = EV-PV)?	-2870
5. What is the calculated Cost Performance Index (CPI = EV/AC)?	0.92
6. What is the cost variance (CV=EV-AC)?	-1110
7. Is the CV% or SV% greater than +/- 10%? (CV%= CV/EV x 100; SV%= SV/PV x 100)	Yes
a. If "yes," was it the?	Both

b. If "yes," explain the variance:

As mentioned in section I.C.2 the TSC attributes variances primarily to the amount of time scheduled for each work package, versus the actual schedule due to uncontrollable requirements from internal and/or external sources that force changes to the product delivery timeline. This is the first FY the TSC has assessed true development, maintenance and enhancement costs, based on the actual receipt of product, with the functionality necessary to increase efficiency. The above totals reflect a rollup of multiple FY06 project DME costs.

c. If "yes," what corrective actions are being taken?

The TSC is working to develop stronger requirement methods that will not interrupt delivery or product or cause changes in the application development. The organization has implemented the process in FY06 for current and future development. Once requirements are "locked", projects will not accept new changes until delivery for the next iteration.

d. What is most current "Estimate at Completion"?	0
8. Have any significant changes been made to the baseline during the past fiscal year?	Yes

8. If "yes," when was it approved by OMB? Yes

Comparison of Initial Baseline and Current Approved Baseline

Milestone Number	Description of Milestone	Initial Baseline		Current Baseline				Current Baseline Variance		Percent Complete
		Planned Completion Date	Total Cost (Estimated)	Completion Date		Total Cost		Schedule (# days)	Cost	
				Planned	Actual	Planned	Actual			
1	TSDB v1.6	12/31/2005	$2.364	12/31/2005	12/31/2005	$2.364	$2.364	0	$0.000	100%
2	EMA v1.8	12/31/2005	$1.576	12/31/2005	12/31/2005	$1.576	$1.576	0	$0.000	100%
3	TSDB v1.7	03/31/2006	$1.272	03/31/2006	03/31/2006	$1.272	$1.272	0	$0.000	100%
4	EMA v1.9	03/31/2006	$1.310	03/31/2006	03/31/2006	$1.310	$1.310	0	$0.000	100%
5	ASP Development	03/31/2006	$1.158	03/31/2006	03/31/2006	$1.158	$1.158	0	$0.000	100%
6	TSDB v1.8	04/24/2006	$1.250	04/24/2006	04/18/2006	$1.250	$1.087	6	$0.163	100%
7	EMA v2.0	06/17/2006	$1.295	06/17/2006	06/17/2006	$1.295	$1.370	0	($0.075)	100%
8	ASP v1.1	08/01/2006	$1.169	08/01/2006	08/01/2006	$1.169	$1.108	0	$0.061	100%
9	TSDB v1.9	07/16/2006	$1.456	07/16/2006	07/16/2006	$1.456	$1.292	0	$0.164	100%
10	EMA v2.1	09/30/2006	$1.495	09/30/2006	09/25/2006	$1.495	$0.987	5	$0.508	100%
11	ASP v1.2	09/30/2006	$1.451	09/30/2006	09/30/2006	$1.451	$0.685	0	$0.766	100%
12	TSS Misc. Development	09/30/2006	$48.203	09/30/2006	09/30/2006	$48.203	$48.203	0	$0.000	100%
13	FY07 TSS Development	09/30/2007	$41.222	09/30/2007		$41.222				0%
14	FY08 TSS Development	09/30/2008	$43.225	09/30/2008		$43.225				0%
15										0%
16										0%
17										0%
18										0%